Exercice 5.

1) On considère les valeurs p = 53, q = 11 et e = 3.
   Reprendre les résultats de l'exercice 3.
2) Bob veut envoyer un message à Alice. Il sait qu'il doit utiliser le système RSA avec les deux entiers n et e. Il transforme en nombres son message en remplaçant par exemple chaque lettre par son rang dans l'alphabet.

   « JEVOUSAIME »

   10 5 22 15 21 19 01 09 13 05

   Puis il découpe son message chiffré en blocs de même longueur (en partant de la droite) représentant chacun un nombre le plus grand possible tout en restant plus petit que n.

   a) Son message devient : 010 052 . . . .
   b) Pourquoi on ne garde pas la longueur 2 des blocs ? Sur quoi on retomberait si on laissait des blocs de 2 ?
   c) Quel message obtient Bob après avoir chiffré chaque bloc ?

      417 . . . .

   d) Quel message retrouve Alice ?

      010 . . . .

Exercice 6.

Connaissant la clé publique (n = 119; e = 5) de ce cryptogramme RSA,

090 086 036 067 032 001 003 031 059 031 :

1. Calculer par tous les moyens p et q.
2. Calculer la clé secrète d.
3. Déchiffrer le cryptogramme.

Exercice 7. Nombres p et q proches

Un programmeur Toto décide de dévier du protocole RSA en choisissant non pas deux grands nombres premiers p et q aléatoires mais deux grands nombres premiers p et q très proches, avec p > q.

1) Supposons que l'entier n soit le produit de deux nombres premiers p et q proches (on peut toujours supposer que p > q). On pose t =$\frac{p+q}{2}$ et s=$\frac{p-q}{2}$. Montrer que :
   a) L'entier s est petit.
   b) n=$t^2 - s^2$.
   c) t est légèrement supérieur à la racine carrée de n.
   d) On peut utiliser ces informations pour déterminer les entiers p et q.
2) Appliquer cet algorithme pour factoriser 899, 110417 et 364957402.
3) Trouver la clé secrète d correspondante à (n = 51983, e = 17).